[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise® 2.6

Cheyenne AVUpdate for InocuLAN Guide

ManageWise®
MANAGEMENT SOFTWARE

Novell®

disclaimer

U.S. GOVERNMENT RESTRICTED RIGHTS

The software and accompanying materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 subdivision (c)(1) and (2), as applicable. Contractor / manufacturer is Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11788-7000 (hereinafter “Computer Associates”).

Computer Associates provides this publication “as is” without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. The entire risk as to the use of this information is assumed by the user.

In no event will Computer Associates be liable for any damages, direct, indirect, incidental, special or consequential, resulting from any defect in the information, even if it has been advised of the possibility of such damages.

Further, Computer Associates reserves the right to revise this publication and to make changes to it from time to time without obligation to notify any person or organization of such revision or change.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries.

Cheyenne is a registered trademark of Computer Associates International, Inc. or one of its subsidiaries.

Other brand or product names used in this manual, but not listed here, are trademarks or registered trademarks of their respective holders.

Credits

Written by Christopher B. Welch

Edited by Alex Chen, Victor Tsui, Thomas Mueller, Carl Oddo, Mark Lewis, Paul Nash, and Stone JyhKwei Shih

Product Support

If you have any questions about this product, please contact us at one of the following:

USA, Canada, Asia, Latin America:	Main Voice Number:	516-465-4000
3 Expressway Plaza	Technical Support:	800-CHEY-TEC
Roslyn Heights, New York 11577		Mon-Fri 8:00 am- 8:00 pm EST
USA		Mon-Fri 8:00 pm-10 pm EST (Callback only)
		Sat/Sun 10:00 am-4:00 pm EST (Callback only)
	Tech Support FAX:	516-465-5115
	BBS:	516-465-3900
	CompuServe:	GO CHEYENNE
	World-wide Web:	http://www.cheyenne.com/
	FTP Server:	ftp.cheyenne.com
	InfoFax System:	516-465-5979 (Outside of North America you must use a fax machine's telephone.)
European Headquarters:	Southern Europe Tech Support:	+33-1-49-93-90-34 Mon-Fri 09:00 - 17:00
Cheyenne Software S.A.R.L.	Tech Support (FAX Hot Line):	+33-1-39-23-18-69
Bel Air Building	BBS:	+33-1-39-23-18-60
58 rue Pottier	Infofax:	+33-1-39-23-47-00
78150 Le Chesnay, France		
Germany:	Central and Eastern Europe Tech Support:	+49-69-920321-80 Mon-Fri 09:00 - 17:00
Cheyenne Software Deutschland	Tech Support FAX:	+49-89-627241-41
Bayerwaldstr. 3	BBS (28800,N,8,1):	+49-89-627241-80
81737 Munich, Germany	BBS ISDN 64kB (v110, v120):	+49-89-627241-85
England:	Northern Europe Tech Support:	+44 (0) 990 239606 Mon-Fri 09:00 - 17:00
Cheyenne Software (UK) LTD	Tech Support FAX:	+44 (0) 990 785783
Furness House	BBS:	+44 (0) 990 143012
53 Brighton Road		
Redhill, Surrey, England RH1 6PZ		
Japan:	Voice:	+81-3-3222-3760
Cheyenne Software K.K.	FAX:	+81-3-3222-3762
Sumitomo Fudosan Sanbancho Bldg.		
3F, 6-26, Sanban-cho, Chiyoda-ku		
Tokyo 102, Japan		
Taiwan:	Voice:	+886-2-545-5611
Cheyenne Software, Taiwan Branch	FAX:	Mon-Fri 9 am- 5 pm
Room C, 4th Floor		+886-2-545-5616
170 Tun Hua North Road		
Taipei, Taiwan		

Training

For the convenience of our customers, Cheyenne University has established a network of Authorized Cheyenne Education Centers and Authorized Cheyenne Instructors. For the latest course descriptions and schedules:

- Customers in U.S./Canada, call: 800-243-9272
- Customers in Europe, Africa, and Middle East, call: +33-1-39-23-18-80
- Customers in Australia, call +61-2-9591944
- Customers in Japan, call: +813-3222-3750
- Customers in Taiwan and Asia, call: +886-2-7951092
- Customers in other areas, call: +1-516-465-4000

CONTENTS

Important Information about this Addendum

InocuLAN AVUpdate for Windows NT

InocuLAN AVUpdate for NetWare

Modifying the AVUpdate.INI file

Preface

IMPORTANT INFORMATION ABOUT THIS ADDENDUM

This document was originally written for the stand-alone InocuLAN product. In this product InocuLAN is bundled with ManageWise and installation and configuration of the AVUpdate software is automatically done for you during the installation of ManageWise. For information on how this is done refer to the ManageWise “Setup Guide”.

The information in this guide is relevant to using AVUpate software on a Windows* NT* server, standalone workstations, reference, and sample purposes only.

1

Chapter

InocuLAN AVUpdate for Windows NT

In this chapter, you will learn about:

Page

AVUpdate for Windows NT Overview

AVUpdate for InocuLAN AntiVirus for Windows NT is a client maintenance program that runs from a login script on a Microsoft Windows NT server or workstation. The AVUpdate program allows you to do the following:

- ➢ automatically install InocuLAN AntiVirus on Windows 95 and Windows 3.x/DOS workstations as users log in to a Windows NT server.
- ➢ automatically updates InocuLAN AntiVirus with the latest program files, updates, and configurations, as the administrator specifies in the AVUPDATE.INI file.

NOTE: If you are using AVUpdate only for updating workstation software, please read "Updating Workstation Software" on page 8.

Understanding the process

Installation files for InocuLAN AntiVirus for Windows NT are kept on a Windows NT server. Modifications are made to the server login script file to run AVUpdate by the server's administrator. The script is assigned to all user accounts that need to have AntiVirus installed.

When a user logs in to the NT domain, the login script runs the AVUpdate program, which will copy the appropriate files (Win 95 or 3.x/DOS) to the workstation and install them. The entire process takes place with no intervention on the user's part, allowing for fully centralized administration. (A workstation re-boot will be needed to activate the AntiVirus real-time scanning. Users will receive a message informing them of this.)

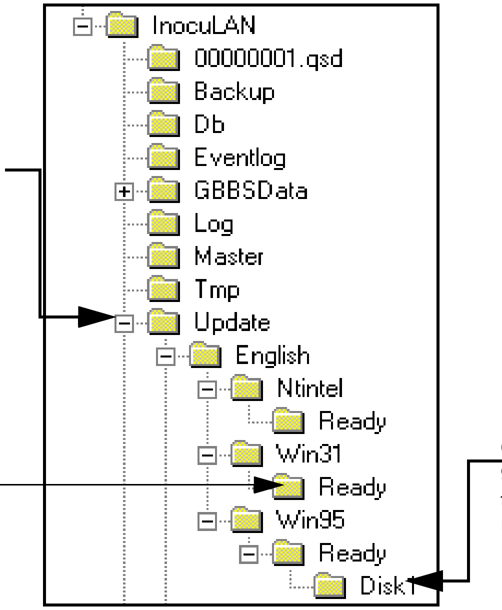
Installing AVUpdate for Windows NT

When you install AVUpdate, you must first set up the program files on your Windows NT machine. Then update the login script in your login script file to specify what machines will receive the files and configurations specified in the AVUPDATE.INI file. Finally, modify the AVUPDATE.INI file to specify exactly what software you want to automatically install on your workstations, what configurations you want to use for InocuLAN AntiVirus for Windows NT.

NOTE: When you install AVUpdate on a server, the AVUPDATE.INI file is initially named AVUPDATE.INO to prevent you from overwriting a customized AVUPDATE.INI file. You can change the name later.

Use the following procedure to configure AVUpdate to install software automatically:

1. The AntiVirus installation files must be properly placed on the server. These files are copied from the AntiVirus CD into the following directories which must be created under the InocuLAN/Update directory:



The Update directory is shared as **cheyupd$** when the InocuLAN service is running. When the service is stopped, the directory is no longer shared.

Run the Windows 3.x setup program and install the program files on the NT server, then copy the files to the following directory: Update\English\Win31\Ready

If you have an AntiVirus CD, copy the Windows 95 installation files to the following directory: Update\English\Win95\Ready\Disk1

NOTE: The example above applies only if you are using InocuLAN AntiVirus 4.0 CD. This is included with the ManageWise CD

If you have previously used the InocuLAN AutoDownload and Distribution feature, some of the above directories may already exist.

Updating the login script file

This line tells Windows NT machines not to run the AVUpdate program.

2. Modify the login script file used on the NT server by adding the following exactly as shown:

```
If "%OS%" == "Windows_NT" goto SKIP
If NOT "%WINBOOTDIR%" == "" goto 95

REM Run AVUpdate using WIN3x syntax
net use v: \\NTSERVER_NAME\cheyupd$
v:\avupdate.exe
net use v: /d
goto SKIP
:95
REM Run AVUpdate using WIN95 syntax
\\NTSERVER_NAME\cheyupd$\
avupdate.exe
:SKIP
```

For the *NTSERVER_NAME* parameter, enter the name of the NT machine set up to be the distribution server. Cheyupd$ is a hidden share that InocuLAN AntiVirus for Windows NT creates on the NT machine to which the workstations will attach. (This share will be removed if the InocuLAN service is stopped or not running.)

NOTE: If you modify a parameters in both your login script and your AVUPDATE.INI file, the command line parameters in the login script supersede the command line parameters in the AVUPDATE.INI file

Modify the AVUPDATE.INI file

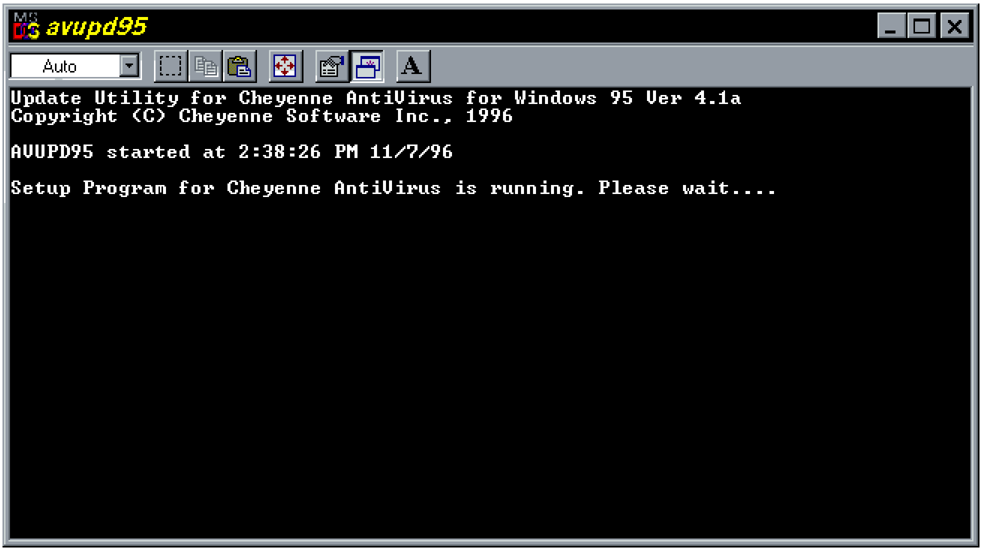
3. Modify the AVUPDATE.INI file, if necessary.

The AVUPDATE.INI file will work without modification. However, to customize the install process, you may want to alter certain parameters. See Chapter 3, “*Modifying the AVUPDATE.INI File*”.

4. Make sure the InocuLAN service is running on the update server. At this point, you may log in to the server and the AVUpdate will run.

Running AVUpdate

When the user logs in to the NT workstation, the login script file will run, launching AVUpdate. A screen similar to the following will appear on the workstation (with operating system specific variations):



```
Update Utility for Cheyenne AntiVirus for Windows 95 Ver 4.1a
Copyright (C) Cheyenne Software Inc., 1996

AVUPD95 started at 2:38:26 PM 11/7/96

Setup Program for Cheyenne AntiVirus is running. Please wait....
```

In Windows 95, a second window will open, showing the files being copied from the server. In Windows 3.x, all processes will be seen in a single window.

All installation options will be run transparently, based on the AVUPDATE.INI file parameters, with no user input required.

When the file copying process completes, users must restart their workstations to finish the installation. Upon restarting, the InocuLAN AntiVirus Real-Time Monitor begins to run, providing real-time virus protection.

Subsequent logins to the server does not re-install InocuLAN AntiVirus. AVUpdate checks for the presence of AntiVirus on the workstation and does not install if a copy already exists.

Once you update AntiVirus files on the NT server (with new virus definitions, for example), AVUpdate automatically updates the workstations with these new files.

Updating Workstation Software

The AVUpdate program automatically updates workstations with new virus signature files as users log in to the NT server.

Signature files are automatically downloaded and placed in the appropriate directories as specified in the `[Distribution]` and `[AutoDownload]` sections of the AVUPDATE.INI file. For details on how to set up and run InocuLAN auto-distribution, please consult the *InocuLAN 4 for Windows NT Guide.*

To set up automatic software updating:

Run the autodownload program

1. Setup and run the InocuLAN for Windows NT automatic download and distribution, as described in the InocuLAN 4 for Windows NT Guide.

   When the download is complete and files have been released for distribution, you are ready to proceed by running AVUpdate.

Update the login script file

2. Modify the login script file used on the NT server by adding the following exactly as shown:

```
If "%OS%" == "Windows_NT" goto SKIP
If NOT "%WINBOOTDIR%" == "" goto 95

REM Run AVUpdate using WIN3x syntax
net use v: \\NTSERVER_NAME\cheyupd$
v:\avupdate.exe
net use v: /d
goto SKIP
:95
```

```
REM Run AVUpdate using WIN95 syntax
\\NTSERVER_NAME\cheyupd$\avupdate.exe
:SKIP
```

For the *NTSERVER_NAME* parameter, enter the name of the NT server set up as the distribution server. Cheyupd$ is a hidden share that InocuLAN AntiVirus for Windows NTcreates on the NT machine to which the workstations will attach.

Modifying the AVUPDATE.INI file

3. Modify the AVUPDATE.INI file, if necessary.

   The default settings in the AVUPDATE.INI file work without modification. However, to customize the install process, you might want to alter certain parameters. For more information on configuring individual settings in your AVUPDATE.INI file, see chapter 3, “*Modifying the AVUPDATE.INI File*”.

4. Make sure the InocuLAN service is running on the NT machine. At this point, you may log in to the NT domain and AVUpdate will run.

NOTE: AVUpdate will check if the files on the server are newer than the files on the workstation. If the files are not new, no update will take place. If the files are new, AVUpdate will automatically copy the new files onto the workstation.

2

Chapter

INOCULAN AVUPDATE FOR NETWARE

In this chapter, you will learn about:

Page

AVUpdate for NetWare Overview

You can configure the AVUpdate program which automatically performs the following functions when you boot up your Windows 95, DOS, or 3.x workstations:

- Install and update new InocuLAN AntiVirus program files and virus signatures.
- Backup the critical disk area on your workstations.
- Configure or modify the operating parameters for your Windows 3.x and 95 clients from the login script or AVUPDATE.INI file.
- Download new virus signatures and AntiVirus program settings for your Windows 3.x and 95 clients during the time window you specify.
- Upload virus scanning records from your Window 3.x and 95 clients.

NOTE: AVUpdate for InocuLAN does not support AntiVirus for NT workstation or InocuLAN for Macintosh.

Automatic Software Installation

The workstation software must reside under the InocuLAN server home directory in order to install the program files on your workstations.

Use one of the following procedures corresponding to your workstation's operating system to automatically install InocuLAN AntiVirus software.

Automatic Software Installation on DOS and Windows 3.x Workstations

1. The Manager MUST be installed on the InocuLAN server.

   a) If you have not previously installed InocuLAN, install InocuLAN to the server.

   Select the *Express* or *Custom* install option.

   b) If the InocuLAN server software has been previously installed, select *Custom Install*. Make sure that *Manager* is the ONLY install option checked.

   NOTE: The DOS and Windows 3.x manager files are written to the MANAGER sub-directory under the InocuLAN home directory. No user intervention is necessary.

   When AVUpdate is executed from the login script, it will copy the files from the `MANAGER` directory or from the HOMEDIR (it will check for the latest file in both directories) to the local workstation drives.

2. If you selected to install the Windows 3.x files, the InocuLAN program group will be created when each workstation loads Windows.

The sample `AVUPDATE.INI` file on page 2-4 shows which parameters (in bold) need to be configured for a Windows 3.x and DOS workstation software installation.

A portion of the AVUPDATE.INI file is presented, below, for reasons of consistency. You need only refer to the sections that are required for the specific platform.

AVUPDATE.INI FOR WINDOWS 3.x and DOS.

```
[Cheyenne InocuLAN AVUpdate]
Path=C:\INOCULAN
Upgrade=Yes
[InocuLAN Windows]
Download=
Install=local
; DOS Program Installation Parameters
[InocuLAN DOS]
Download=
Install=local
; AUTOEXEC.BAT Configuration for DOS and Windows 3.x
Installation
[Autoexec]
SetEnv=yes
Examine=yes
Immune=yes
```

NOTES:
1) The platform-specific settings are shown, in bold, on the next two pages.
2) For descriptions of each AVUPDATE.INI parameter see Chapter 3, Modifying the AVUPDATE.INI File.

2. When you are ready for AVUpdate to install your clients, you incorporate the following lines into your login script:
   MAP <drive letter>:=<servername/volume:>
   #<drive letter>:\INOCULAN\AVUPDATE
   <options>.

Windows 95 Workstations

1. Create a sub-directory under the InocuLAN home directory called **DOWNLOAD\95**.

NOTE: The DOWNLOAD directory may already exist under the InocuLAN home directory unless the user has the original signature files from the original release of the program.

2. Create an additional sub-directory under **DOWNLOAD\95\DISK1**.

   The directory will hold the Windows 95 workstation manager files to be installed by AVUpdate.

NOTE: Users of client 1.0 will also need to create an additional directory called DISK2.

3. Copy the InocuLAN 95 installation disk(s) or CD to directory created in step 2.

4. When AVUpdate is executed, on a Windows 95 machine, it invokes the Setup program in the DISK1 sub-directory.

The portions of the AVUPDATE.INI file shown on pages 2-6 and 2-7 show which parameters (in bold) need to be configured for a Windows 95 workstation software installation.

NOTE: When using the Microsoft client make sure that the First Network Drive setting is NOT the same drive letter that AVUpdate is using in the login script.

The portions of the AVUPDATE.INI file necessary for updating Windows 95 workstations are presented on the following pages. You need only refer to the sections that are required for the specific platform.

AVUPDATE.INI FOR WINDOWS 95.

```
; Cheyenne for Windows 95 Parameters and User Information
[UserInfo]
FullName=Cheyenne AntiVirus
CompanyName=Cheyenne Software, a Division of Computer Associates
[LicenseInfo]
CDKey=CXX1X14CXXX9XMM7XHY
[InocuLANInstall]
InocuLANPath=
RebootAfter=0
RebootTimeout=3
ScanAfter=0
[Components]
Manager=1
Service=1
Realtime=1
bNetwareSupport=0
OverwriteRegistry=1
Uninstall=1
GetBBS=0
;Windows 95 Distribution Settings
[Distribution]
PrimaryServer=<Name of the NT Server>
DaysOfWeek=127
NoTimeLimit=1
BeginHour=0
BegMinute=0
EndHour=0
EndMinute=0
Timeout=240
[Startup]
AutoDownloadAgent=0
SchedualedScanAgent=1
bStartJob=0
[Internet Integration]
Explorer=0
Navigator=0
```

NOTES:
1) The platform-specific settings are shown, in bold.
2) For descriptions of each AVUPDATE.INI parameter see Chapter 3, “Modifying the AVUPDATE.INI File”.
3) The distribution section only applies to NT servers distributing updates to clients.

5. When you are ready to install AVUpdate to your clients, you incorporate the following lines into your login script:

```
MAP <drive letter>:=<servername/volume:>
#<drive letter>:\INOCULAN\AVUPDATE
<options>
```

NOTE: This portion of the AVUPDATE.INI file might not contain some settings that you will see in the complete file.

AVUpdate Client Requirements for NetWare

This section provides guidelines to automatically install AVUpdate software to the workstations.

Before you can update your workstations, you should be familiar with the following requirements:

1. Windows NT Clients cannot be installed/updated with AVUpdate. The client software can be obtained from Cheyenne BBS or Compuserve (GO CHEYENNE) and installed manually from the following files.

   IL0080.ZIP - for NetWare, DOS, and Windows 3.x

   IL0082.ZIP for Windows 95

2. When a Windows 95 workstation is using the Microsoft client for NetWare networks, make sure that the First Network Drive setting is NOT the same drive letter that AVUpdate is using in the login script.

3. Do NOT delete the drive mapping.

4. Do NOT remap the AVUpdate drive letter.

NOTE: Previous versions of InocuLAN documentation use the format of `#SERVERNAME/VOL:\HOME_DIRECTORY\AVUPDATE.EXE` in the installation examples. This syntax is no longer supported.

Protecting the Critical Disk Area

AVUpdate performs a virus scan before backing up the critical disk area, the area vulnerable to virus infection. When a user logs in, the system login script runs AVUpdate, which checks for a backup of the critical disk area. If the critical area backup does not exist, AVUpdate will perform the backup. This backup can be used by any of the InocuLAN, DOS, or Windows client programs to restore the Critical Disk Area.

Please refer to you InocuLAN Supervisor Guide for more information on the Critical Disk Area.

NOTES: AVUpdate requires a minimum of 363K Conventional Memory to backup critical disk area. AVUpdate loads the virus signature data and scans the critical disk files before backing up the critical disk area.

Updating Workstations

The workstation software update process is automated when `AVUPDATE.EXE` is executed from the user's login script. It requires some preparation on the part of the network administrator.

There are three steps to prepare the server for the workstations to receive the new InocuLAN files:

1. Retrieve the software updates from the http://www.cheyenne.com, Cheyenne BBS [516-465-3900], or from Compuserve (GO CHEYENNE).

   The latest software update files are:

   NetWare/DOS/Windows 3.x: `IL0080.ZIP`

   Windows 95: `IL0082.ZIP`

   The installation procedures for each of the files are available with their accompanying `README.TXT` files.

2. Copy the contents of the appropriate platform's zip file to the associated directories.

   - For Windows 3.x and DOS:
     Copy the unzipped contents of the IL0080.ZIP file to the MANAGER sub-directory under the InocuLAN home directory.
   - For Windows 95:
     Copy the unzipped contents of the IL0082.ZIP file to the DOWNLOAD\95 sub-directory under the InocuLAN home directory.

   AVUpdate will copy these files to the InocuLAN workstation home directory.

3. Add the following lines to the system login script:

   MAP <*drive letter*>:=<*servername/volume:*>

   #<*drive letter*>:\INOCULAN\AVUPDATE <*options*>

NOTE: These lines will be present if you used AVUpdate to automatically install your software.

AVUpdate Security Rights

This chart lists the rights for the three main InocuLAN directories. These must be set appropriately to ensure proper AVUpdate operation.

	Rights				
Directory	**[R]ead**	**[W]rite**	**[C]reate**	**[E]rase**	**Scan [F]iles**
INOCULAN\CRITICAL.WS	✓	✓💾	✓		✓
INOCULAN HOME DIRECTORY	✓				✓
INOCULAN\MASTER DIRECTORY	✓	✓💻	✓💻	✓💻	✓
INOCULAN\MANAGER DIRECTORY	✓				✓

💾 = If backing up to the Critical Disk Area to a server. If the individual users are members of a group then that group must ALSO include the ***Create, Write***, and ***Erase*** rights.
💻 = If uploading scan records or installing the manager to the server.

AVUpdate Configuration Methods

Use the following methods to set AVUpdate parameters:

Recommended Configuration Method

- ➢ Set the update parameters for your system based upon its operating system using the AVUPDATE.INI file. You may specify separate AVUPDATE.INI files for different groups of users when using the F= command line parameter. (Please refer to Chapter 3, Modifying the AVUPDATE.INI File.)
- ➢ By specifying command line parameters in your login script. Please refer to the "AVUpdate Command Line Parameters" section on page 3-49.

Configuring AVUpdate for Windows 95

AVUpdate will update files of any compatible InocuLAN AntiVirus product or client that is installed on the same workstation. For more information about the supported clients, see page 2-2 of this chapter.

To prevent the AVUpdate window from remaining open after the processing is completed:

➢ Check the InocuLAN home directory and locate `AVUPDATE.PIF` (included with this ZIP file). If this file does not exist, create a PIF file or ‘shortcut file’ in the InocuLAN home directory called `AVUPDATE.PIF`. Make sure the *Close on Exit* option on the *Program* tab is enabled.

To prevent the user from seeing the AVUpdate processing screen:

➢ Change AVUPDATE.PIF to the *Run Minimize* option.

The user might see a minimized icon on the application tray. The window, itself, does not appear.

Uploading Virus Scan Records

Each time a virus scan is performed on a workstation a local scan log (*.REC files) is created on the workstation. An InocuLAN scan database (MASTER.DB) is also kept on the InocuLAN server and on the workstation in order for the network administrator to access the completed workstation scanning records.

Each time a user logs into the network, AVUpdate compares the date of the local workstations scan log to the date of the server's scan master log database. If the workstation's log is newer the newest records are copied to the InocuLAN server's master database.

NOTE: If disk space is a concern on the InocuLAN server, you might want to keep the Upload Scan records function disabled.

To ensure that InocuLAN server has the latest scan records:

- ➢ Edit `AVUPDATE.INI` on the InocuLAN server and make sure that UploadScan Records=YES. This option is disabled by default.
- ➢ Make sure the user's rights are set properly. For more information about required user rights, refer to the chart on page 2-11.

Configuring AVUpdate for Multiple Groups of Users

AVUpdate can be used to install and update multiple groups of users with different configurations. While the system login script can be used to parse individual login names (using *%LOGIN_NAME*), it is recommended that the users be put into groups.

Here is a sample system login script that uses AVUpdate to run two different installs/updates:

```
MAP F:= NY_MARKETING/SYS:
IF MEMBER OF "MANAGERS"THEN #F:\INOCULAN\AVUP-
   DATE F=AVUPMNGR.INI
ELSE
#F:\INOCULAN\AVUPDATE F=AVUPDATE.INI
END
```

The above example checks to see if the user is a member of the group named *MANAGERS*. If that user is a member then `AVUPDATE.EXE` will initialize following the commands specified in `AVUPMNGR.INI`. If the user is not a member of the *MANAGERS* group, then `AVUPDATE.EXE` will use its default `AVUPDATE.INI` file. These group can refer to different platforms. For instance, one user group could be assigned to a DOS/ Windows 3.x section and the other can be assigned to Windows 95.

NOTES:

1. If no INI parameter file is specified, when using AVUPDATE.EXE from a command line or login script, the AVUPDATE.INI default settings are used.

2. After performing an installation for the first time, a file ALSO named AVUPDATE.INI is created on the workstation’s local hard disk. This file matches the file on the server if the server’s files have been changed to create a new configuration. Although this file is also named AVUPDATE.INI, this file is not identical to the AVUPDATE.INI file in the InocuLAN server’s home directory. Thus, you should not overwrite the file on the server.

3. AVUPDATE.INI, located on the users workstation, should not be modified or deleted unless instructed to do so by Support Personnel. This file is used each time a user logs in and runs AVUPDATE.EXE.

4. Regardless of what file name the “F=” AVUPDATE.EXE command line parameter is set to, the workstation’s file is still named AVUPDATE.INI.

Examples of AVUpdate Operation

Here are two scenarios that helps you understand how AVUpdate operates:

- Protecting workstations running both DOS and Windows 3.x
- Running Windows 3.x from a network.

Protecting DOS and Windows 3.1x Workstations

In this first example, you as the network administrator, want to safeguard the workstations on your network by putting AVUpdate in the system login script. We will assume that you purchased InocuLAN for NetWare and installed client software and the server software on a server named NY_MARKETING.

After reading the InocuLAN Supervisor’s Guide, you have chosen to install the Real-Time Monitors Immune TSR and WImmune VxD on the your workstations and maintain backups of their Critical Disk Areas.

1. Start by using a text editor to open the file AVUPDATE.INI located in the server directory to which you installed InocuLAN.

   (If you used the default, this will be NY_MARKETING/SYS:\INOCULAN.)

2. Add the following settings to the configuration (your additions are marked in bold.):

3. Next add AVUpdate to the system login script for NY_MARKETING by adding the following lines:

   ```
   MAP F:=NY_MARKETING/SYS:
   #F:\INOCULAN\AVUPDATE
   ```

NOTE: Previous versions of InocuLAN documentation use the format of #servername/ vol:\home_directory\AVUPDATE.EXE in their installation examples. This is syntax is no longer supported.

4. The next time a users logs into NY_MARKETING, the following screen is displayed on the screen:

```
Updated 7 Files on Workstation
Testing Extended Memory...OK
Loading Virus Signature File ... OK
Examining Workstation Memory ... OK
No Viruses Were Detected In Workstation Memory
Checking for Boot Viruses On Drive [C] ...
No Boot Viruses Detected.
Scanning file C:\IO.SYS ...OK
Scanning file C:\MSDOS.SYS ...OK
Scanning file C:\COMMAND.COM ...OK

Back Up Destination: C:\INOCULAN\

      CMOS Settings: C:\INOCULAN\CMOS.SIG
    Partition Table: C:\INOCULAN\PARTSECT.SIG
        Boot Sector: C:\INOCULAN\BOOTSECT.SIG
   BIOS System File: C:\INOCULAN\BIOS.SIG
    DOS System File: C:\INOCULAN\DOS.SIG
     DOS Shell File: C:\INOCULAN\SHELL.SIG
   Information File: C:\INOCULAN\INFO.SIG
    C:\AUTOEXEC.BAT: C:\INOCULAN\AUTOEXEC.SIG
      C:\CONFIG.SYS: C:\INOCULAN\CONFIG.SIG



Checking for Boot Viruses On Drive [C] ...
No Boot Viruses Detected.
Scanning file C:\IO.SYS ...OK
Scanning file C:\MSDOS.SYS ...OK
Scanning file C:\COMMAND.COM ...OK

Back Up Destination: NY_MARKETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\
     CMOS Settings: ...RKETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\CMOS.SIG
   Partition Table: ...ING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\PARTSECT.SIG
       Boot Sector: ...ING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\BOOTSECT.SIG
  BIOS System File: ...RKETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\BIOS.SIG
   DOS System File: ...ARKETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\DOS.SIG
    DOS Shell File: ...KETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\SHELL.SIG
  Information File: ...RKETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\INFO.SIG
   C:\AUTOEXEC.BAT: ...ING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\AUTOEXEC.SIG
     C:\CONFIG.SYS: ...ETING/SYS:\INOCULAN\CRITICAL.WS\000c0329.a71\CONFIG.SIG

   Backup Successful!!!
```

NOTE: The location of the Critical Disk Area Backup is based on the network address of the workstation.

For DOS/Windows 3.x Workstations:

The next time the workstation is booted, the Immune TSR will be loaded into memory. The next time Windows is run, the InocuLAN Active Monitor will be started.

For Windows 95 Workstations:

AVUpdate will cause the InocuLAN for Windows 95 Setup program to run in the background without any user interaction.

The Setup Program will take care of copying the files and writing the information to the Windows 95 Registry. It will then reboot the machine to complete the setup and run the Active Monitor.

For ALL Workstations:

Upon subsequent logins, only the following will appear on the screen (assuming the software on the server has not been updated, and the workstation and Critical Disk Area Backup are still intact):

```
Copyright (C) Cheyenne Software, Inc.
      1996. All rights reserved.
AVUPDATE V4.0 -- InocuLAN Automatic
      Update Program ---
```

Running AVUpdate for Windows 3.x from the Network

There are two methods available for putting AVUpdate in a login script for organizations that choose to have their workstations run Windows 3.x from a network drive. AVUpdate finds the individual’s Windows INI files - `WIN.INI` and `SYSTEM.INI`.

Method 1: This method sets up a temporary drive mapping and passes it to AVUpdate using the `/WI` parameter.

```
MAP F:= NY_MARKETING/SYS:
MAP ROOT G:= NY_MARKETING/SYS:\US-
   ERS\%LOGIN_NAME\WIN31
#F:\INOCULAN\AVUPDATE /WI=G:\
```

Method 2: This method sets up a search drive to the user’s INI files. AVUpdate will find them in the path.

```
MAP INS S16:=NY_MARKETING/VOL1:\NETWIN
MAP INS S16:=NY_MARKETING/SYS:\US-
   ERS\%LOGIN_NAME\WIN31
MAP H:=NY_MARKETING/SYS:
# H:\INOCULAN\AVUPDATE
```

InocuLAN BBS Update Files

This section lists the files mentioned throughout this document. The filenames will remain the same although their contents will be updated as new versions become available. Many of the filenames remain the same for backward compatibility.

File Name	Description
`IL0080.ZIP`	Signature update for NetWare, DOS, and Windows 3.x platforms.
`IL0082.ZIP`	Signature update for Windows 95 platform.
`IL0084.ZIP`	Signature update for the Windows NT. Versions of this file exist for all of the platforms Windows NT runs on. For example, IL0084i.ZIP = Windows NT for Intel. However, AVUpdate for NetWare does not use this file.
`IL0135.ZIP` ✓	Contains the latest revision of AVUPDATE.EXE.

Further information about these files and others, for InocuLAN and Cheyenne AntiVirus, are available through the Cheyenne BBS [516-465-3900] and from our forum on Compuserve [GO CHEYENNE].

NOTE: Each file contains a `README.TXT` file that explains the update and/or installation process.

3

Chapter

MODIFYING THE AVUPDATE.INI FILE

In this chapter, you will learn about:

Configuring the AVUPDATE.INI File

The `AVUPDATE.INI` is a text file used to set the following operation parameters for InocuLAN AntiVirus clients on your network:

- When and how often your clients download software and/or virus signatures from your InocuLAN servers
- What program files are distributed from servers to clients on your network
- The settings and options for setting up and running InocuLAN AntiVirus on your workstations

NOTE: For more descriptions and definitions of settings for a parameter, refer to the comments in the AVUPDATE.INI file and the INOCULAN.ICF file, which are preceded by a semicolon.

The AVUPDATE.INI File

Here is an example of the default AVUPDATE.INI file. You may modify the settings to suit the needs of the workstations in your enterprise. For a description of the purpose of each individual setting, see the following section, AVUPDATE.INI Parameters.

AVUpdate Parameters

```
[Inoculan AVUpdate]
UpdateLevel=1
UploadScanRecords=
Windows3xIniPath=
Path=C:\INOCULAN
Delete=
Upgrade=Yes

[Critical Disk Backup]
Local=
Server=

; Windows 3.x Parameters
[InocuLAN Windows]
Download=
Install=yes
Upgrade95=yes
Domain=

[Wimmune]
Install=yes

[AMScanOptions]
InfctAct=0
ReNameExt=AVB
ChangeConfiguration=
CustomMessage=
Message=
Direction=
```

Continued....

```
ProtectFloppy=
ProtectNetWork=
ScanExeOnly=
ScanMode=
ScanArchives=
ArcExtName=ZIP*ARJ*
DosFileFilter=*.*
ExtName=APP*BIN*COM*DLL*DRV*EXE*OVL*OVR*
PRG*SYS*VXD*
SkipExtName=

[ScanOptions]
ShowSplash=
ChangeConfiguration=
ExtName=
Interactive=
BeepOnDetect=
ScanExeOnly=
ScanBoot=
ScanFiles=
InfctAct=
ScanMode=
ScanCompressedFiles=
CompressedExtName=ARJ*ZIP*
ScanArchives=
ArcExtName=ARJ*ZIP*
ReNameExt=AVB
DosFileFilter=
DoMappingDrive=
GenerateScanRec=
CustomMessage=
Message=
```

Continued....

```
[InocuLAN DOS]
Download=
Install=
[Immune]
Install=
Options=

[Autoexec]
SetEnv=yes
Examine=yes
Immune=
CommandLineScan=
ScanOptions=

[Examine]
Install=yes
Options=

[InocuLAN 95]
Download=HomeDir\Download\95
SetupPath=HomeDir\Download\95\Disk1
ExcludeDOSManager=Yes
Run=AVUP95LD.EXE

[UserInfo]
FullName=InocuLAN AntiVirus
CompanyName=Cheyenne, a Div. of Computer
Associates

[LicenseInfo]
bFromCDKey=1
CDKey=CXXX1X14CXXX9XMI7XJY
LicenseFile=
```

Continued....

```
[InocuLANInstall]
InocuLANPath=
RebootAfter=0
RebootTimeout=3
ScanAfter=0

[Components]
Manager=1
Service=1
Realtime=1
bNetwareSupport=0
OverwriteRegistry=1
Uninstall=1
GetBBS=0

[Distribution]
PrimaryServer=
SecondaryServer=
DaysOfWeek=127
NoTimeLimit=1
InBegHr=0
InBegMin=0
InEndHr=0
InEndMin=0
Timeout=240
```

Continued....

```
[Startup]
AutoDownloadAgent=0
SchedualedScanAgent=1
bStartJob=0

[Internet Integration]
Explorer=0
Navigator=0

[RealTime]
ExeOnly=1
Method=0
Mode=1
Direction=3
bFloppyDrive=1
bNetworkDrive=1
bFloppyBoot=1
CompFiles=ZIP*ARJ*LHA*LZH*MIM*UUE*
ExclFiles=BTR*DBF*SBF*DB*MDB*MDX*NDX*
ExeFiles=APP*BIN*COM*DLL*DOT*DOC*DRV*EXE
*OVL*OVR*PRG*SYS*VXD*XLT*XLA*XLS*XLW*
ScanCompressed=1
skipCDROM=0
SuspendTime=0
```

Continued....

```
[LocalScanner]
Interactive=1
BeepOnDetect=1
ScanExeOnly=0
ScanArchives=1
ScanBoot=1
ScanFiles=1
InfctAct=0
ScanMode=1
AutoDisplay=1
ExtName=APP*BIN*COM*DLL*DOT*DOC*DRV*EXE*
OVL*OVR*PRG*SYS*VXD*XLT*XLA*XLS*XLW*
SkipExtName=BTR*DBF*SBF*DB*MDB*MDX*NDX*
ArcExtName=ZIP*ARJ*LHA*LZH*MIM*UUE*
CopyInfectionReport=0

[AutoDownload]
ConnectionMethod=2
NextDownloadDate=
NextDownloadTime=
DownloadTime=20:00
DownloadOnDay=17
SkipMonths=1
FtpHostName=ftp.cheyenne.com
FtpUserEMailAddress=somebody@somecompany
.com
FtpUserName=anonymous
FtpFastConnection=0
```

AVUPDATE.INI Parameters

The operating parameters are explained in the following tables and are presented in the order that they shown in the above template.

[Inoculan AVUpdate]		
Parameter	**Default**	**Purpose**
UpdateLevel=<number>	1 (If this value is higher than that of the workstations' AVUPDATE.INI file, the update will be executed.)	Determines whether AVUpdate will do a file-by-file comparison of workstation and server files.
UploadScanRecords=<yes or no> For NetWare - UploadScanRecords=<yes or no> For NT - UploadScanRecords=<no>	NONE For NT - ALWAYS "NO"	If the value is "YES", the workstation's scan records will be uploaded to the server.
Windows3xIniPath= For NT - NEVER USE	NONE	This setting applies to Windows 3.x and DOS. This parameter lists the path to WIN.INI and SYSTEM.INI on the network server which runs Windows 3.x. Refer to the /WI switch listed on page 3-49.
Path=<drive/dir>	C:\INOCULAN	Force installation to this path (DOS and Windows 3.x only). If directory does not exist, it will be created.
Delete=<Yes or No>	NONE For NT - Always NO	For NetWare - If YES, obsolete files will be deleted (from InocuLAN 3.0) as indicated in AVUPDATE.DAT.
Upgrade=<yes or no> For NetWare - Upgrade=<Yes or No> For NT - Server=<NO>	NONE For NT - Always NO	Indicate "NO" to prevent AVUpdate from upgrading a workstation running InocuLAN version 3.0 to InocuLAN version 4.0.

[Critical Disk Backup]		
Parameter	**Default**	**Purpose**
Local=<Yes-or-No>	NONE	YES creates a Critical Disk Area Backup on the workstations' local hard drive.
Server=<Yes or No>	NONE For NT - Always NO	YES creates Critical Disk Area Backup on the server.

[InocuLAN Windows]		
Parameter	**Default**	**Purpose**
Download=	NT default - (Do not change) Download=HOMEDIR\English\Win31\Ready NetWare default - NONE NOTES: 1. If this is left blank or set equal to NONE, AVUpdate checks the InocuLAN home directory and the manager directory. 2. The DOWNLOAD directory may already exist under the InocuLAN home directory unless the user has the original signature files from the original release of the program.	Indicates the path of the AntiVirus program files and updates. Indicates to AVUpdate that this is the current InocuLAN directory. Thus, HOMEDIR must be part of the indicated path. Do not change the path to reflect *drive letter\InocuLAN*.

[InocuLAN Windows]		
Parameter	**Default**	**Purpose**
Install= NT default - Install=<Yes or No> NetWare default - Install=<Server or Local>	YES If NONE, will not install	For NT - Select *Yes* to install InocuLAN for Windows, select *NO* if you do not want to install it. For NetWare - *Local* indicates the workstation will have InocuLAN for Windows installed on its local drive. *Server* indicates that an icon will be set up to run the program from the server. NOTE: The Windows workstation sub-directory must be in the search path.
Upgrade95=<Yes or No>	For NT - YES For NetWare - YES (AntiVirus for Windows 95 is not installed if AntiVirus for Windows 3.x already exists.)	YES is used only for Windows 95 workstations that already have InocuLAN for Windows 3.x installed. Selecting YES will upgrade the 3.x software to Win 95 software. “NO” will NOT install InocuLAN for Windows 95 if InocuLAN for Windows 3.x is already installed on the workstation.
Domain= For NT - Domain=<No> For NetWare - Domain=<Yes or No>	For NT - ALWAYS “NO”	Distributes the Domain Manager DLL to workstations.

Continued...

[Wimmune]		
Parameter	**Default**	**Purpose**
Install= For NT - Install=<Yes or No> For NetWare - Install=<Server or Local>	YES (will not install)	Local or Yes indicates the workstation will have InocuLAN for Windows installed on its local drive.

Continued from previous page

[AMScanOptions]		
Parameter	**Default**	**Purpose**
InfctAct=<0 through 7>	0	Enter a value to specify the action your Windows 3.x Active Monitor takes when it detects a virus. “0” - A report is generated and sent to persons you specify. “1” - The file is deleted. “2” - The file is renamed with the.AVB extension. Subsequent files with the same initial characters are sequentially renamed.AV0, .AV1, .AV2, etc. “3” - The file is cured. “4” - The file is moved to the *virus* subdirectory of the InocuLAN home directory. “5” - The infected files are destroyed utterly. “6” - The file is moved to the *virus* subdirectory of the InocuLAN home directory and renamed with the .AVB extension. Subsequent files with the same initial characters are named sequentially with the extensions .AV0, .AV1, .AV2, etc. “7” - The original file is copied and then cured.

Continued...

[AMScanOptions]		
Parameter	**Default**	**Purpose**
ReNameExt=	.AVB	Enter an extension to use for renamed files. We suggest that you leave this one alone.
ChangeConfiguration=<0 or 1>	0	Enter a value to specify whether or not you want to allow users to change the configuration. “0” - Users cannot change the configuration. “1” - Users are able to change the configuration.
CustomMessage=<0 or 1>	0	Enter a value to specify whether or not you want to create customized messages. “0” - Customized messages are not created. “1” - Customized messages are created.
Message=	Your customized message to indicate that a virus has been detected.	Enter your customized message to indicate that a virus has been detected. For example, “Virus detected. Please call the MIS department.”

[AMScanOptions]		
Parameter	**Default**	**Purpose**
Direction=<0, 1, 2, or 3>	3	Enter a value to specify whether or not you want to protect incoming files, outgoing files, or both. “0” - The Active Monitor is disabled. “1” - Incoming files are protected. “2” -Outgoing files are protected. “3” - Both incoming and outgoing files are protected.
ProtectFloppy=<0 or 1>	0	Enter a value to specify whether or not you want the Active Monitor to scan your floppy drives when the diskette is read. “0” - The diskette is not scanned. “1” - The diskette is scanned.
ProtectNetwork=<0 or 1>	0	Enter a value to specify whether or not you want mapped network drives to be scanned in real time by the Active Monitor. “0” - Network drives are not scanned by the Active Monitor. “1” - Network drives are scanned by the Active Monitor.

Continued...

[AMScanOptions]		
Parameter	**Default**	**Purpose**
ScanExeOnly=<0, 1, 2, 3, or 4>	0	Enter a value to specify whether you want to scan executable files with default extensions only, all files save those with the default executable extensions, or all files. "0" - All files are scanned. "1" - Scans specified extensions only. "2" - Scans all files save those with the specified extensions. "3" - Scans all files types that match the definition specified in the DosFileFilter section. "4" - Scans only executable files.
ScanMode=<0, 1, or 2>	0	Enter a value to specify what type of scan job you want the Active Monitor to perform 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns). Note: Review scans may give false warnings of virus detection.

[AMScanOptions]		
Parameter	**Default**	**Purpose**
ScanArchives=<0 or 1>	0	Enter a value to specify whether or not you want the Active Monitor to scan compressed files. “0” - Compressed files are not scanned. “1” - Compressed files are scanned.
ArcExtName=	ZIP*ARJ*	Enter all of the extensions for the types of compressed files you want the Active Monitor to scan.
DosFileFilter=	*.*	Specify the wildcard for target files. (Use with the ScanExeOnly command line mentioned in this section.)
ExtName=	APP*BIN*COM*DLL*DRV*EXE*OVL*OVR*PRG*SYS*VXD*	Enter the file extensions for the default types of executable files.
SkipExtName=		Specify the extensions for the types of files that you want to skip in scan jobs in your Active Monitor.

[Scan Options]

Parameter	Default	Purpose
ShowSplash=<0 or 1>	1	Enter a value to specify whether or not to display the Splash Screen by default. "0" - The Splash Screen is not displayed. "1" - The Splash Screen is displayed.
ChangeConfiguration=<0 or 1>	0	Enter a value to specify whether or not you want to allow users to change the configuration. "0" - Users cannot change the configuration. "1" - Users are able to change the configuration.
ExtName=		Enter the file extensions for the default types of executable files.
Interactive=<0 or 1>	0	Enter a value to specify whether or not to prompt users when a virus is detected. "0" - Users are not prompted when a virus is detected. "1" - Users are prompted when viruses are detected.

Continued...

[Scan Options]		
Parameter	**Default**	**Purpose**
BeepOnDetect=<0 or 1>	0	Enter a value to specify whether or not your computer provides an audible warning when a virus is detected. “0” does not generate an audible warning. “1” generates an audible warning.
ScanExeOnly=<0, 1, or 2>	0	Enter a value to specify whether you want to scan executable files with default extensions only, all files save those with the default executable extensions, or all files. “0” - All files are scanned. “1” - Scans specified extensions only. “2” - Scans all files save those with the specified extensions. “3” - Scans all files types that match the definition specified in the DosFileFilter section. “4” - Scans only executable files.
ScanBoot=<0 or 1>	0	Enter a value to specify whether or not to scan the boot sector area of your hard disk. “0” - the boot sector is not scanned “1” - the boot sector is scanned.

[Scan Options]		
Parameter	**Default**	**Purpose**
ScanFiles=<0 or 1>	1	Enter a value to specify whether or not to scan the DOS files on your local drive. “0” - DOS files are not scanned. “1” - DOS files are scanned.

[Scan Options]		
Parameter	**Default**	**Purpose**
InfctAct=<0 through 7>	0	Enter a value to specify the action your Windows 3.x Active Monitor takes when it detects a virus. “0” - A report is generated and sent to persons you specify. “1” - The file is deleted. “2” - The file is renamed with the .AV extensions. Subsequent files with the same initial characters are sequentially renamed .AV0, .AV1, .AV2, etc. “3” - The file is cured. “4” - The file is moved to the *virus* subdirectory of the InocuLAN home directory. “5” - The infected files are destroyed utterly. “6” - The file is moved to the *virus* subdirectory of the InocuLAN home directory and renamed with the .AVB extension. Subsequent files with the same initial characters are named sequentially with the extensions .AV0, .AV1, .AV2, etc. “7” - The original file is copied and then cured.

[Scan Options]		
Parameter	**Default**	**Purpose**
ScanMode=<0, 1, or 2>	0	Enter a value to specify what type of scan job you want the Active Monitor to perform 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns).
ScanCompressedFiles=< 0 or 1>	0	Enter a value to specify whether or not you want to scan compressed files. (for DOS 4.0) “0” - Compressed files are not scanned. “1” - Compressed files are scanned.
CompressedExtName=	ARJ*ZIP*	Enter the file extensions for the types of compressed files you want to scan.
ScanArchives=<0 or 1>	0	Enter a value to specify whether or not you want to scan compressed files. (for DOS 5.0) “0” - Compressed files are not scanned. “1” - Compressed files are scanned.

[Scan Options]		
Parameter	**Default**	**Purpose**
ArcExtName=	ARJ*ZIP*	Enter the file extensions for the types of compressed files you want to scan.
ReNameExt=	.AVB	Enter an extension to use for renamed files.
DosFileFilter=		Specify the wildcard for target files. (Only use if ScanExeOnly=3.)
DoMappingDrive=<0 or 1>	0	Enter a value to specify whether or not to include the NetWare Drives in the directory tree. “0” - The NetWare drives are not included in the directory tree. “1” - The NetWare drives are included in the directory tree.
GeneratesScanRecord=< 0 or 1>	0	Enter a value to specify whether or not to generate a scanning record files. (These files can only be generated when you are running the Server Manager.) “0” - Scanning record files are not generated. “1” - Scanning record files are generated.

[Scan Options]		
Parameter	**Default**	**Purpose**
CustomMessage=<0 or 1>	0	Enter a value to specify whether or not you want to create customized messages. "0" - Customized messages are not created. "1" - Customized messages are created.
Message=	Your customized message to indicate that a virus has been detected.	Enter your customized message to indicate that a virus has been detected. For example, "Virus detected. Please call the MIS department."

[InocuLAN DOS]		
Parameter	**Default**	**Purpose**
Download=HOMEDIR\<path> NOTE*: HOMEDIR*\ is used, by InocuLAN, to indicate the directory from which AVUpdate is run.	NONE NOTES: 1. If this is left blank/ NONE, AVUpdate will check the InocuLAN home directory and the manager directory. 2. The DOWNLOAD directory may already exist under the InocuLAN home directory unless the user has the original signature files from the original release of the program.	Indicates the path from where to copy AnitiVirus program files and updates. Indicates to AVUpdate that this is the current InocuLAN directory. Thus, HOMEDIR must be part of the indicated path. Do not change to reflect *drive letter\InocuLAN.*

Continued...

[InocuLAN DOS]

Parameter	Default	Purpose
Install=<Server or Local> For NT - Install=<Local>	NONE (will not install)	Indicates whether the workstation will have InocuLAN for DOS installed on the local drive.

[Immune]

Parameter	Default	Purpose
Install=<Yes or No>	NONE	YES will install and run Immune TSR through the workstations' AUTOEXEC.BAT file.
Options=	NONE	This passes any command line parameters to Immune TSR when it is run via the AUTOEXEC.BAT file.

Continued from previous page.

[Autoexec]		
Parameter	**Default**	**Purpose**
SetEnv=<Yes or No>	YES	"YES" adds the line "SET INOCULAN=<*InocuLAN install path*>' to the AUTOEXEC.BAT file. "NO" removes the line from the AUTOEXEC.BAT file.
Examine=<Yes or No>	Yes	"Yes" passes any command line parameters to Immune TSR when it is run in the AUTOEXEC.BAT file. "No" removes the line from the AUTOEXEC.BAT file.
Immune=<Yes or No>	NONE	"YES" adds Immune TSR to the AUTOEXEC.BAT file. "No" removes the line from the AUTOEXEC.BAT file.
CommandLineScan= <Yes or No>	NONE	"YES" adds INOCUCMD.EXE to the AUTOEXCE.BAT file. "No" removes the line from the AUTOEXEC.BAT file.
ScanOptions=	NONE	This passes any command line parameters to EXAMINE when it is run from the AUTOEXEC.BAT file.

[Examine] Common to DOS, Windows 3.x, and Windows 95		
Parameter	**Default**	**Purpose**
Install=<Yes or No>	Yes	YES copies EXAMINE.EXE file to the workstation but will not be added to the Autoexec.bat unless specified in the [Autoexec] sub-section. The Examine parameter is set to YES.

[Examine]
Common to DOS, Windows 3.x, and Windows 95

Parameter	Default	Purpose
Options= For example, to set EXAMINE to use quiet mode and not to check the CMOS setup, the Options line would be set as follows: Options=/Q /S	NONE	This passes additional command line parameters to EXAMINE when it is run in the AUTOEXEC.BAT file. The parameters are: /C - Creates a new Critical Disk backup on the workstation. Does NOT backup the server. /A - Accept all changes found. /R - Restore changes to original state. /I - Ignore changes. /1 - Check Upper memory area. /N - No memory check. /S - No checking of the CMOS Setup. /Q - Quiet mode. /L - Use local (home) directory and not environment symbol.

[InocuLAN 95]		
Parameter	**Default**	**Purpose**
Download=	For NT - Download=HOMEDIR\English\Win95\Ready For NetWare - Download=HOMEDIR\Download\95 NOTE*: HOMEDIR*\ is used, by InocuLAN, to indicate the directory from which AVUpdate is run. NOTES: 1. If this is left blank/ NONE, AVUpdate will check the InocuLAN home directory and the manager directory. 2. The DOWNLOAD directory may already exist under the InocuLAN home directory unless the user has the original signature files from the original release of the program.	Indicates the path from where to copy AntiVirus program files and updates. Indicates to AVUpdate that this is the current InocuLAN directory. Thus, HOMEDIR must be part of the indicated path. Do not change to reflect *drive letter\InocuLAN.*

SetupPath=	For NT -
	SetupPath=HOMEDIR\English\Win95\Ready\Disk1
	For NetWare -
	Setup=HOMEDIR\Download\95\Disk1
		Indicates the path from which the setup program is run. Indicates to AVUpdate that this is the current InocuLAN directory. Thus, HOMEDIR must be part of the indicated path. Do not change to reflect *drive letter\InocuLAN.*

[InocuLAN 95]		
Parameter	**Default**	**Purpose**
ExcludeDOSManager=<yes-or-No>	Yes	Overrides the ‘Install=’ setting in the [InocuLAN DOS] section when installing software on the Windows 95 Workstations. If YES is specified the DOS Manager is NOT installed.
Run=AVUP95LD.EXE	RESERVED. DO NOT CHANGE.	Not Applicable.

[User Info]		
Parameter	**Default**	**Purpose**
FullName=	InocuLAN AntiVirus	Defines the registered user’s name.
CompanyName=	Cheyenne, a Division of Computer Associates	Defines the registered company’s name.

<table>
<tr><th colspan="3"><code>[License Info]</code></th></tr>
<tr><th>Parameter</th><th>Default</th><th>Purpose</th></tr>
<tr><td>bFromCDKey=<0, 1, or 2&gt;</td><td>1</td><td>Enter a value to specify which license is used when AVUpdate searches for license information.
“0” - Use the license file specified in the “LicenseFile=” parameter.
“1” - Use the CD key if InocuLAN AntiVirus is not installed, otherwise use the license file from the existing installation.
“2” - For CD key installation. Do not use dashes.</td></tr>
<tr><td>CDKey=</td><td>CXXX1X14CXXX9XMI7XJY - Live Trial CD key</td><td>20 digit CD key.</td></tr>
<tr><td>LicenseFile=</td><td>License file in the setup directory</td><td>Enter the name of the License file.</td></tr>
</table>

<table>
<tr><th colspan="3"><code>[InocuLANInstall]</code></th></tr>
<tr><th>Parameter</th><th>Default</th><th>Purpose</th></tr>
<tr><td>InocuLANPath=</td><td>NONE - will install the program files into the directory, C:\Program Files\InocuLAN\AntiVirus, or update the current directory.</td><td>Indicates the path for installation of InocuLAN for Windows 95.</td></tr>
</table>

[InocuLANInstall]		
Parameter	**Default**	**Purpose**
RebootAfter=<0 or 1>	0.- Do not change this value.	
RebootTimeout=<0>	0 - Do not change this value.	Enter a value for the period of time (in minutes) after which your workstation reboots.
ScanAfter=<0>	0 - Do not change this value.	Enter a value to specify whether or not to run a scan after AVUpdate has run. "0" - The virus scan will not run. "1" - The virus scan runs.

[Components]		
Parameter	**Default**	**Purpose**
Manager=<1 or 0>	1 (Manager will be installed)	To specify whether or not AVUpdate will install the Workstation Scanner.
Service=<1 or 0> - The value must agree with the RealTime parameter below.	1 (Real Time device driver and Manager will be installed)	To specify whether or not AVUpdate will install the Real Time device driver and Manager (Windows NT).
RealTime=<1 or 0> - The value must agree with the Service parameter above.	1 (Real time Scanning Monitor will be installed)	To specify whether or not AVUpdate will install the Real Time device driver (Windows 95 & 3.x).

[Components]

Parameter	Default	Purpose
bNetwareSupport=<1 or 0>	0 (NetWare Domain Manager is not installed)	To specify whether or not AVUpdate will install the NetWare Domain Manager.
OverwriteRegistry=<1 or 0>	1 (Previous settings are overwritten)	To specify whether or not AVUpdate will overwrite previous registry settings.
Uninstall=<1 or 0>	1 (installs the uninstall program)	To specify whether or not AVUpdate will install the uninstall components.
GetBBS=<1 or 0>	0 (the AutoDownload Agent and Manager are not installed)	“1” installs the AutoDownload Agent and Manager.

[Distribution Settings]

Parameter	Default	Purpose
PrimaryServer=	None	Name of the remote InocuLAN Server to obtain UPDATE program files from. (For NT only)
SecondaryServer=	None	Name of the second remote InocuLAN to get the update from if the primary server does not have one of its own. (For NT only)

[Distribution Settings]		
Parameter	**Default**	**Purpose**

DaysOfWeek=<0x0001=1 through 0x0040=64>	127	Use the following decimal values (in conjunction with beginning and ending hour and minute values), representing the individual days of the week or combination of days, to specify a period for distributing/updating InocuLAN AntiVirus program files:
		`0x0001=1 (Sunday)`
		`0x0002=2 (Monday)`
		`0x0004=4 (Tuesday)`
		`0x0008=8 (Wednesday)`
		`0x0010=16 (Thursday)`
		`0x0020=32 (Friday)`
		`0x0040=64 (Saturday)`
		`0x0007F=127 (all days)`
		Note: You can specify two days by adding the values of the decimals.

NoTimeLimit=<1 or 0>	1 (indicates no time limit for downloading or updating your InocuLAN AntiVirus program files)	"1" specifies a limited time period for downloading and updating your InocuLAN AntiVirus program files.

[Distribution Settings]		
Parameter	**Default**	**Purpose**
BeginHour=<0-23>	“0” (12:00 AM)	The hour determining when distribution is to begin. The range is 0 (12:00 AM) through 23 (11:00 PM)
BegMinute=<0-59>	“0” (1 minute)	The number of minutes past BeginHour indicating when distribution is to begin. The range is 0 through 59.
EndHr=<0-23>	“0” (12:00 AM)	The hour determining when distribution is to end. The range is 0 (12:00 AM) through 23 (11:00 PM)
EndMinute=<0-59>	“0” (1 minute.)	The number of minutes past EndMinute indicating when distribution is to end. The range is 0 through 59
Timeout=<240>	240 (minutes)	Indicates a value (in minutes) for a period of time in which to query for a distribution of software updates or virus signatures.

[Startup]		
Parameter	**Default**	**Purpose**
AutoDownloadAgent=<1 or 0> Does not apply if the GetBBS parameter in the [Components] section equals “0”.	0 (indicates that the AutoDownload agent will not run when you boot up your machine)	“1” indicates that you will automatically download new virus signatures from Cheyenne’s ftp site or BBS when you boot up your machine.
SchedueledScanAgent=<1 or 0>	0 (indicates that the Scheduled Scan Agent will not run when you boot your machine)	“1” indicates that the Scheduled Scan Agent will run a scheduled scan when you boot up your machine.
bStartjob=<1 or 0>	0 (indicates that a startup job will not occur)	“1” indicates that a scan job will run when you boot up your workstation.

[Internet Integration] Warning: These settings will erase all zip file associations if installed.		
Parameter	**Default**	**Purpose**
Explorer=<1 or 0>	0	Enter a value to specify whether or not to integrate AVUpdate with the Microsoft Internet Explorer. “0” - AVUpdate is not integrated with Explorer. “1” - AVUpdate is integrated with Explorer.

[Internet Integration] **Warning: These settings will erase all zip file associations if installed.**		
Parameter	**Default**	**Purpose**
Navigator=<1 or 0>	0	Enter a value to specify whether or not to integrate AVUpdate with the Netscape Navigator browser. “0” - AVUpdate is not integrated with Netscape. “1” - AVUpdate is integrated with Netscape.

[Real Time]		
Parameter	**Default**	**Purpose**
ExeOnly=<0, 1, or 2>	1	Enter “0” to scan all files, “1” to scan files with the default extensions, or “2” to scan all files save those with the default extensions.

[Real Time]		
Parameter	**Default**	**Purpose**
Method=<1 through 7>	0	You select from one of the following actions upon detection of viruses: 0 - Report only 1 - Delete the infected file 2 - Rename the file with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, AV2, etc. 3 - Copies infected files to a temporary directory, then cures the file in the original location. 4 - Moves files to a temporary directory. 5 - Purges the files from your local drives destroying them utterly. 6 - Moves infected files from the original directories to a temporary directory and renames the files with the .AV* extension (subsequent files with the same initial characters will be named.AV0, .AV1, AV2, etc.

[Real Time]		
Parameter	**Default**	**Purpose**
Mode=<0, 1, or 2>	1	You specify one of three scanning methods to use when AVUpdate scans your local drives: 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns)
Direction=<0, 1, 2, or 3>	3	Enter a value to specify whether to scan incoming or outgoing files on your hard drive: 0 - The Real Time monitor is disabled 1 - Outgoing files are scanned. 2 - Incoming files are scanned. 3 - Both incoming and outgoing files are scanned.
bFloppyDrive=<0 or 1>	1	Enter a value to specify whether or not to scan floppy disks before you access files on them. “0” does not scan the floppy drive. “1” scans the floppy drive.

[Real Time]		
Parameter	Default	Purpose
bNetworkDrive=<0 or 1>	1	Enter a value to specify whether or not to scan mapped network drives before you access files on them. “0” does not scan the network drive. “1” scans the network drive.
bFloppyBoot=<0 or 1>	1	Enter a value to specify whether or not to scan the boot sectors of all floppy disks before your floppy drive accesses them. “0” does not scan the boot sector of the floppy disk. “1” scans the boot sector of the floppy disk.
CompFiles=	ZIP*ARJ*LHA*LZH*MIM*UUE*	Enter the extensions for the compressed files you want to scan separated by a “*”. Note: You are only allowed to specify 20 extensions.
ExclFiles=	BTR*.DBF*SBF*DB*MDB*MDX*NDX*	Enter the extensions for the files you want to exclude from your scans when you boot up your workstation. Note: You are only allowed to specify 20 extensions.

[Real Time]		
Parameter	**Default**	**Purpose**
ExeFiles=	APP*BIN*COM*DLL*DOT*DOC*DRV*EXE*OVL*OVR*PRG*SYS*VXD*XLT*XLA*XLS*XLW*	Enter the extensions for all of the files used to execute programs (used for fast scans). Note: You are only allowed to specify 20 extensions.
ScanCompressed=<0 or 1>	1	Enter a value to specify whether or not to scan compressed files. “0” = NO “1” = YES
SkipCDROM=<0 or 1>	0	Enter a value to specify whether or not to scan the CD-ROM using Real Time scanning “0” = NO “1” = YES.
SuspendTime=	0	Enter a value (in seconds) for the number of seconds of suspensions allowed for Real Time scanning.

`[Local Scanner]`		
Parameter	**Default**	**Purpose**
Interactive=<0 or 1>	1	Enter a value to specify whether or not the user is prompted to take action when a virus is detected. "0" does not prompt you to take action. "1" prompts you to take an action.
BeepOnDetect=<0 or 1>	1	Enter a value to specify whether or not your computer provides an audible warning when a virus is detected. "0" does not generate an audible warning. "1" generates an audible warning.
ScanExeOnly=<0, 1, or 2>	0	Enter a value to specify whether to scan all files, executable files with default extensions, or all files save executable files with default extensions. "0" will scan all files. "1" scans executable files with default extensions. "2" scans all files save executable files with default extensions.

[Local Scanner]		
Parameter	**Default**	**Purpose**
ScanArchives=<0 or 1>	1	Enter a value to specify whether or not the Local Scanner scans compressed files. “0” does not scan compressed files. “1” scans compressed files.
ScanBoot=<0 or 1>	1	Enter a value to specify whether or not to scan the boot sector area of your hard disk. “0” - the boot sector is not scanned “1” - the boot sector is scanned.
ScanFiles=<0 or1>	1	Enter a value to specify whether or not to scan only the boot sector area of your hard disk. “0” - files are scanned. “1” - only the boot sector is scanned.

[Local Scanner]		
Parameter	**Default**	**Purpose**
InfctAct=<0 through 6>	0	Enter a value to specify what actions are taken on infected files by the local scanner. 0 - Report only 1 - Delete the infected file 2 - Rename the file with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, AV2, etc. 3 - Copies infected files to a temporary directory, then cures the file in the original location. 4 - Moves files to a temporary directory. 5 - Purges the files from your local drives destroying them utterly. 6 - Moves infected files from the original directories to a temporary directory and renames the files with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, AV2, etc.

[Local Scanner]		
Parameter	**Default**	**Purpose**
ScanMode=<0, 1, or 2>	0	Enter a value to specify what type of scan the Local Scanner uses: 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns).
AutoDisplay=<0 or 1>	1	Enter a value to specify whether or not the results dialog is displayed after the scan job is performed. “0” - does not display the results dialog box. “1” - displays the results dialog box.
ExtName=	“APP*BIN*COM*DLL*DOT*DOC*DRV*EXE*OVL*OVR*PRG*SYS*VXD*XLT*XLA*XLS*XLW*”	Lists of the types executable file types by extension that are scanned by the Local Scanner.
SkipExtName=	“BTR*DBF*SBF*DB*MDB*MDX*NDX*”	Lists of the types executable file types by extension that are not scanned by the Local Scanner.
ArcExtName=	ZIP*ARJ*LHA*LZH*MIM*UUE*	Enter a value to specify the different types of compressed files (by type) the Local Scanner scans.

[Local Scanner]		
Parameter	**Default**	**Purpose**
CopyInfectionReport=<0 or 1>	0	Enter a value to specify whether or not the Local Scanner produces the Copy Infection Report, which is generated from the Scan Log Record (.REC) file. “0” - The Copy Infection Report is not generated. “1” - The Copy Infection Report is generated.

[Auto Download]		
Parameter	**Default**	**Purpose**
ConnectionMethod=<1 or 2>	2	Enter a value to specified the desired connection method for downloading program files or virus signatures.
NextDownloadDate=<mm/dd/yy>	Blank - The next download will be executed one month after the Autodownload was first executed.	Enter a date in the mm/dd/yy format to specify when the next download is to occur.
NextDownloadTime=<hh:mm>	Blank - The next download will be executed on the time that the first Autodownload was executed.	Enter a time using the hh:mm format (Ex. 18:00 = 6:00 P.M.) to specify the time when the next download should be executed.

[Auto Download]		
Parameter	**Default**	**Purpose**
DownloadTime=<hh/ mm>	20:00 (8:00 P.M.)	Enter a time using the hh:mm format to specify when a download should occur.
DownLoadOnDay=<digits for a day of the month>	17	Enter a value to specify a day of the month on which to download virus signatures or program files.
SkipMonths=<number of months to skip between downloads>	1	Enter a value to specify the interval (in months) to skip between downloads.
FtpHostName=<the URL for the FTP site>	ftp.cheyenne.com	Enter the URL for the ftp site from which you want to download program files and/or virus signatures.
FtpUserEmailAdress=	<somebody@ somecompany.com>	Enter the e-mail address for users' workstations. If a proxy server is used, the user might need to provide a password for it.
FtpUserName=<the user name for an ftp session>	"anonymous"	Enter the user name for your ftp sessions.
FtpFastConnection=<0 or 1?	0	Enter a value to specify that your workstation has a fast internet connection. "0" - There is no fast internet connection. "1" - A fast internet connection exists.

[NEC PC-98]		
Parameter	**Default**	**Purpose**
Configuration=avupnec.ini	Do not change.	Since NEC PC's are not fully IMB compatible, you must specify a special .INI file for installing, configuring, or upgrading InocuLAN AntiVirus programs.l
FileList=avupnec.ini	Do not change.	Specifies the files for upgrading or configuring your AntiVirus or InocuLAN program files on the NEC PC-98 platform.

Editing the AVUPDATE.INI File

There is ONLY one `AVUPDATE.INI` file for all supported platforms. You can edit the lines in this file for the parameters that apply to the operating system you are running with a text editor.

AVUpdate Command Line Parameters

The following command line parameters are used as a supplement to the `AVUPDATE.INI` configuration file.

AVUpdate Command Line Parameter Settings	
Option	**Description**
`H or ?`	`Displays current configuration and help parameters.`

`Q`	`Quiet Mode enabled as a default.`
	`This setting is provided for backward compatibility with older versions.`

`Q- or`
`V[erbose]`
	`Prompt user before any updates are made. Asks for a key press before ending the update session.`

F=<*IniFile*>	`Specifies the AVUpdate configuration file. The overrides the default name of AVUPDATE.INI.`

AVUpdate Command Line Parameter Settings	
Option	**Description**
U	Upload workstation scan record to the server. This will send the current workstation scan records to the server, where it can be viewed by the domain manager. Using this option gives the network supervisor a centralized record of all workstation scanning activities.
WI= <*path*>	Use to indicate the path to Windows 3.x INI files. This is needed only when running Windows from a Network Server.
W	Adds the group setup loading information to the Windows WIN.INI file. The program manager group setup will be executed and automatically create InocuLAN group and icons in Windows 3.x when the load Windows after the install has been completed. No files will be installed to the workstation.

AVUpdate Command Line Parameter Settings	
Option	**Description**
WL	Loads Windows Local client software. AVUpdate will determine if it is running Windows 3.1x or Windows 95. Under Windows 3.1x the Group Setup Program will create all the icons when Windows is first loaded after the install. Under Windows 95 the special Windows 95 setup program is executed.
DOS	Loads InocuLAN for DOS. AUTOEXEC.BAT is modified is necessary.
A	**AUTOEXEC.BAT OPTIONS**: X - Do not modify V - Set Environment variable (default) E - Include Examine.exe (default) I - Include Immune.exe (default with ID option) S - Include InocuCMD.exe (option defaults to "*") Sample: AVUPDATE **AX** or AVUPDATE **AVEI**
IF	Loads Immune Full which includes immune.exec and wimmune.exe. The AUTOEXEC.BAT and SYSTEM.INI files are modified if necessary.

AVUpdate Command Line Parameter Settings	
Option	**Description**
ID	Loads Immune for DOS. AUTOEXEC.BAT is modified is necessary.
EX	Loads Examine. AUTOEXEC.BAT is modified is necessary.
IW	Load Immune for Windows (wimmune.exe) WIN.INI and SYSTEM.INI files modified if necessary.
P=<*path*>	Install Path. This overrides the current environment variable setting, if any, and the AUTOEXEC.BAT file will be modified with the new environment string. The order of the path selection, during the installation, is: 1. Current environment variable setting 2. C:\INOCULAN (if nothing else specified).
CDS	Runs Critical Disk Backup to the server.
CDL	Runs a Critical Disk Backup to a workstations local drive.
DEL	Deletes InocuLAN version 3.0 files.

For example, if you want the DOS client and Wimmune VxD to be installed on the workstation when AVUpdate is run you would type, at the DOS prompt or following “#” in a login script:

```
    AVUPDATE /D /IW
  (“/” is only valid for NetWare 3.x)
```

INDEX